

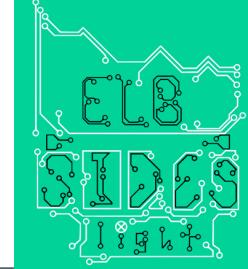
# A beginner's guide to SSO (mis)configuration

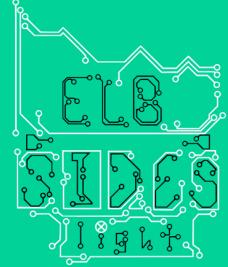
Elbsides Light 2023  
2023-11-17  
Adina Bogert-O'Brien

# What exactly am I going to talk about?

## Covered

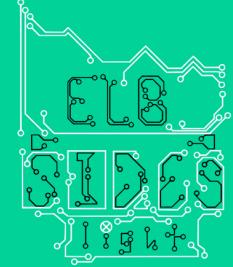
- Making sure a **vendor's SSO** offering **works for your business**





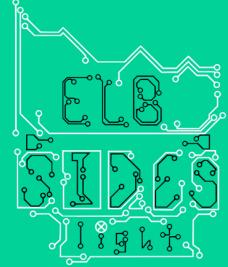
# Why am I giving this talk?

**Bad SSO can make you feel safe,  
while hiding vulnerabilities**



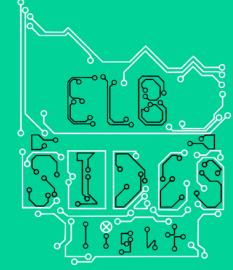
# Why am I giving this talk?

**Empower yourself and your colleagues  
to ask questions!**



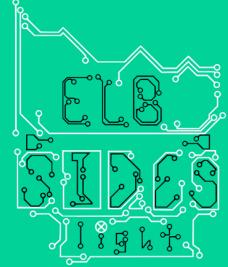
# What the heck is SSO anyway?

And why does your company want it?

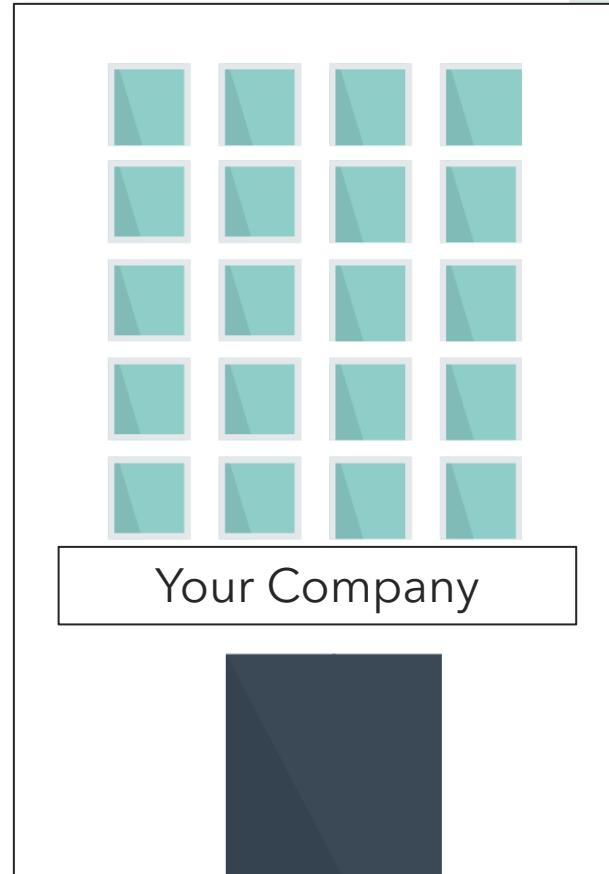


**Single sign-on (SSO)** is an authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.

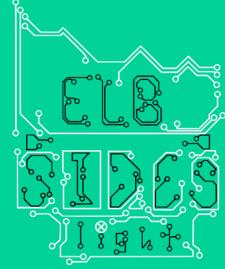
Wikipedia contributors, "Single sign-on", Wikipedia, The Free Encyclopedia, 14 November 2023



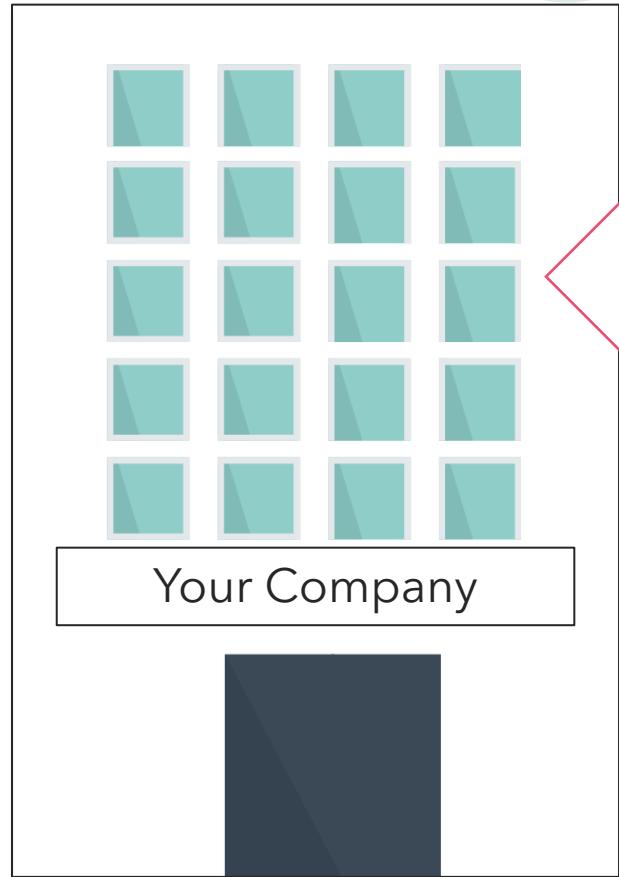
# Your company in the past: under control



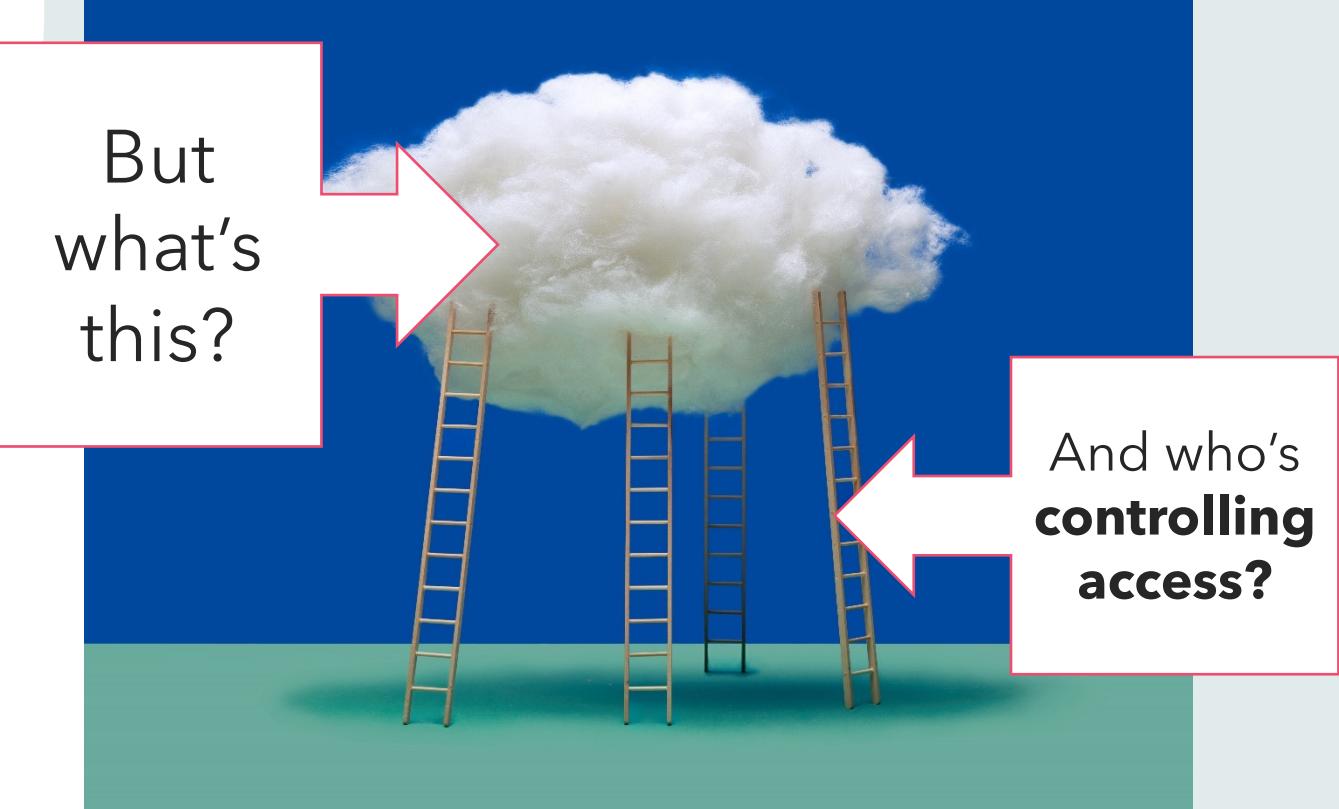
All your stuff  
is in  
**your systems**



# Your company now: a cloudy mess

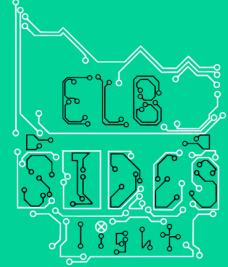


**Some**  
stuff is  
still  
here



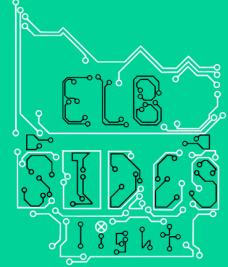
But  
what's  
this?

And who's  
**controlling**  
**access?**



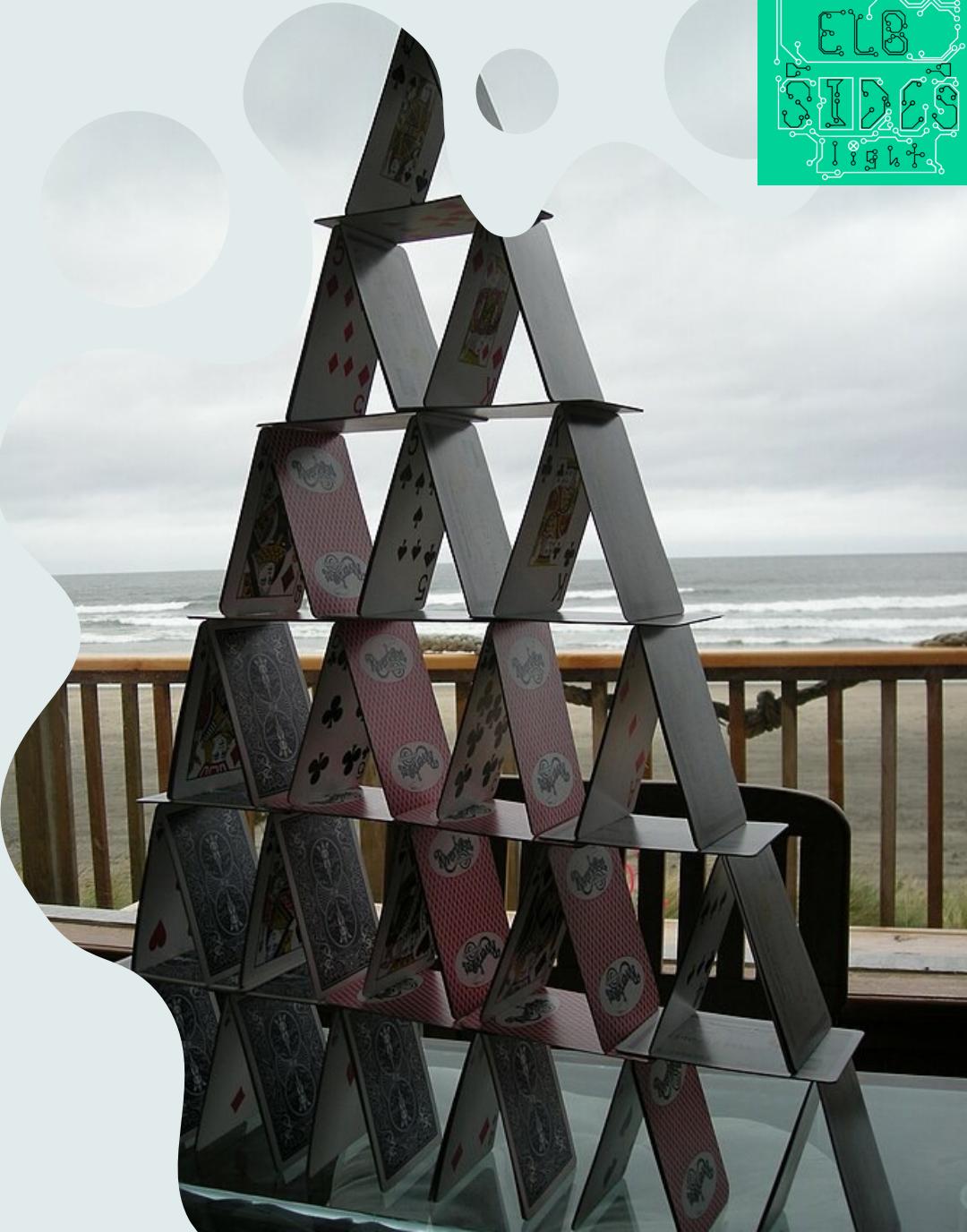
Vendor stuff





# The dream

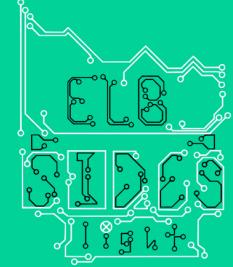
- **centralize** managing users
- **make life easier** for your colleagues
- enforce consistent **security standards**



# The reality

- SSO protocols are just **a way** for your company's Identity Provider **to tell your vendor "Yeah, that's Bob"**



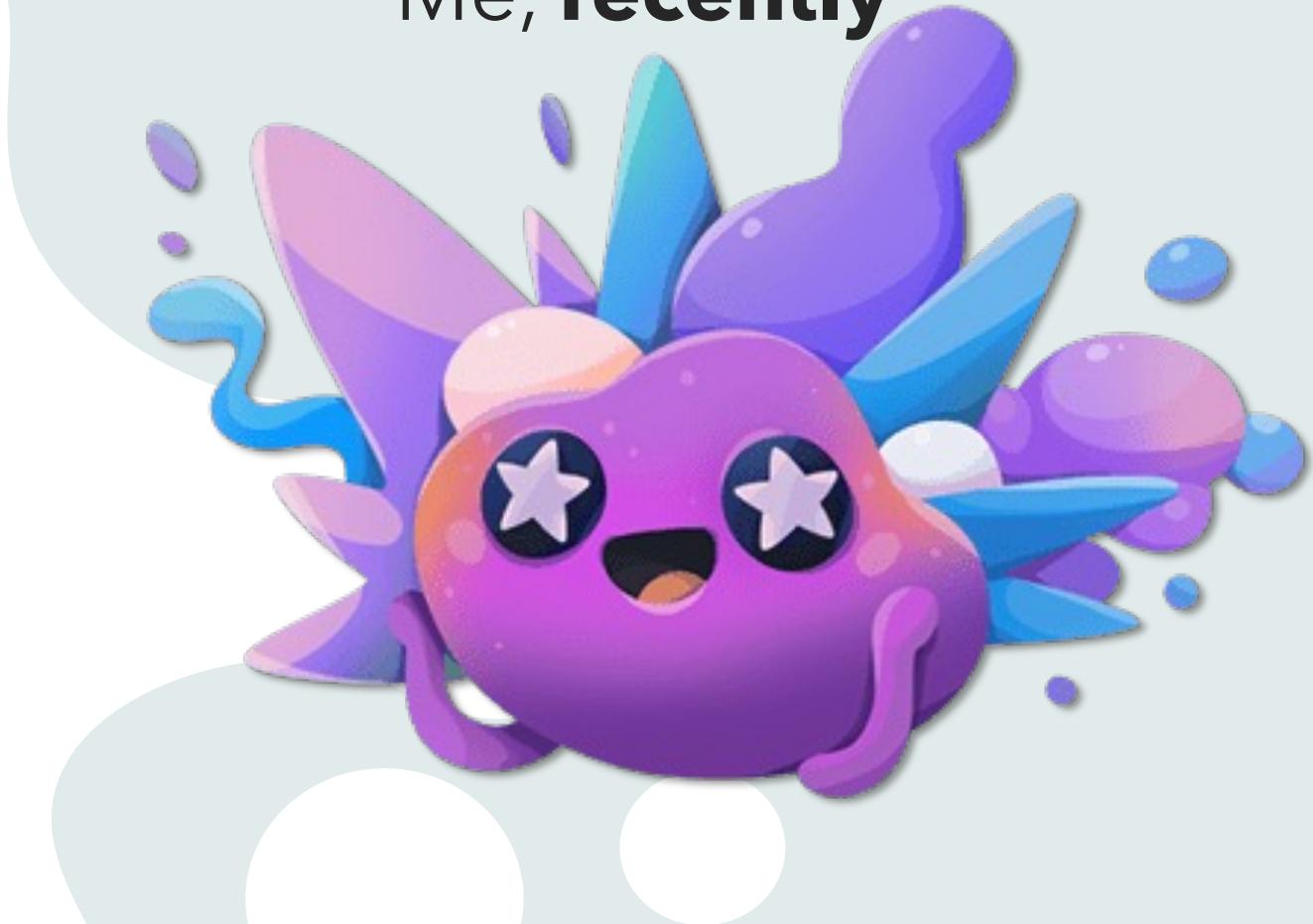


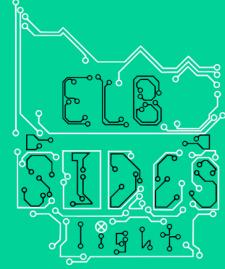
# Why am I giving this talk?

## Step 1: **Idealism**

- SSO is good!
- My vendors offer SSO
- I'll **just turn it on** and ***everything will be fine***

Me, **recently**





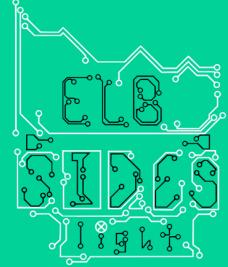
# Why am I giving this talk?

## Step 2: **OMG WTF SSO**

- What do I actually **need**?
- **What** can my vendor **do**?
- **Ask weird questions:**  
communication is hard and  
people make mistakes

Me, **now**





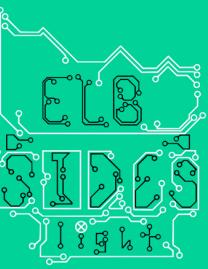
# Why am I giving this talk?

## Step 2: **OMG WTF SSO**

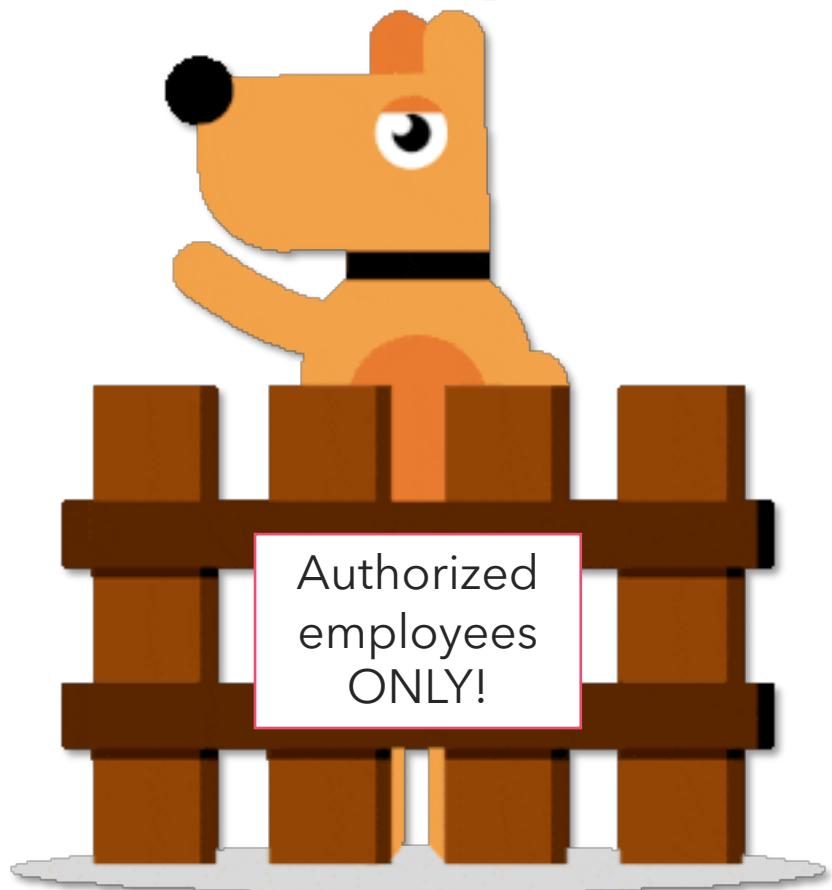
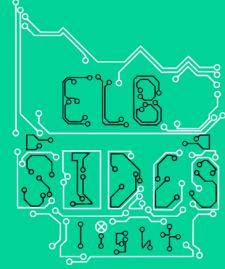
- What do I actually **need**?
- **What** can my vendor **do**?
- **Ask weird questions:**  
communication is hard and  
people make mistakes

Me, **now**





My company's needs

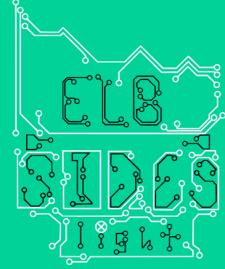


## Need #1: Use my authentication

My company's needs



Need #2: Users  
can **only access**  
their **own** stuff



# Why am I giving this talk?

## Step 2: **OMG WTF SSO**

- What do I actually **need**?
- **What** can my vendor **do**?
- **Ask weird questions:**  
communication is hard and  
people make mistakes

Me, **now**



# SSO doesn't come first (or even third)

They're building a Cool New Internet Thing!

SSO comes wayyyy later, thanks to pesky customers.



When they do  
build SSO

They have  
**different**  
**ideas** about  
SSO than  
you!



## Create your account

Note that phone verification may be required for signup. Your number will only be used to verify your identity for security purposes.

Email address

Continue

Already have an account? [Log in](#)

OR



Continue with Google

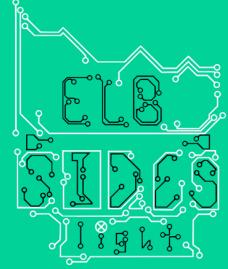


Continue with Microsoft Account

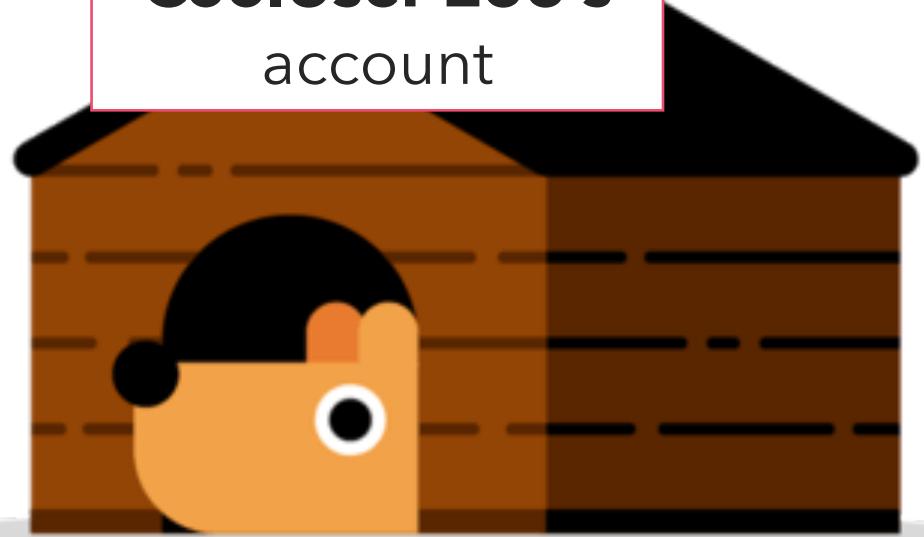


Continue with Apple

Maybe they want  
to **allow SSO**,  
but **not force it**

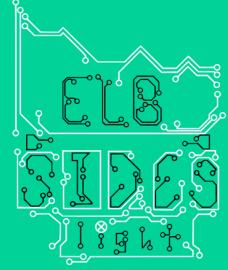


**CoolUser 256's**  
account



Bob, and only Bob

They might not  
care about  
usernames  
matching

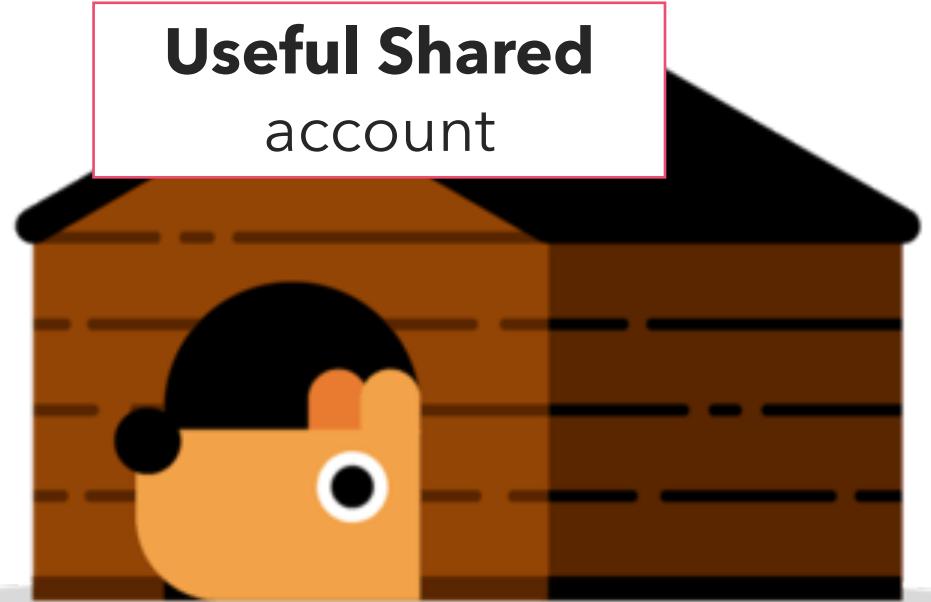
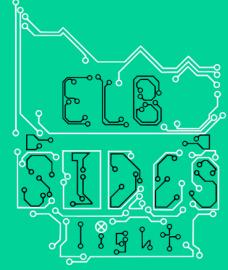


CoolUser 256's  
**BEsT BoB's**  
account



Bob, and only Bob

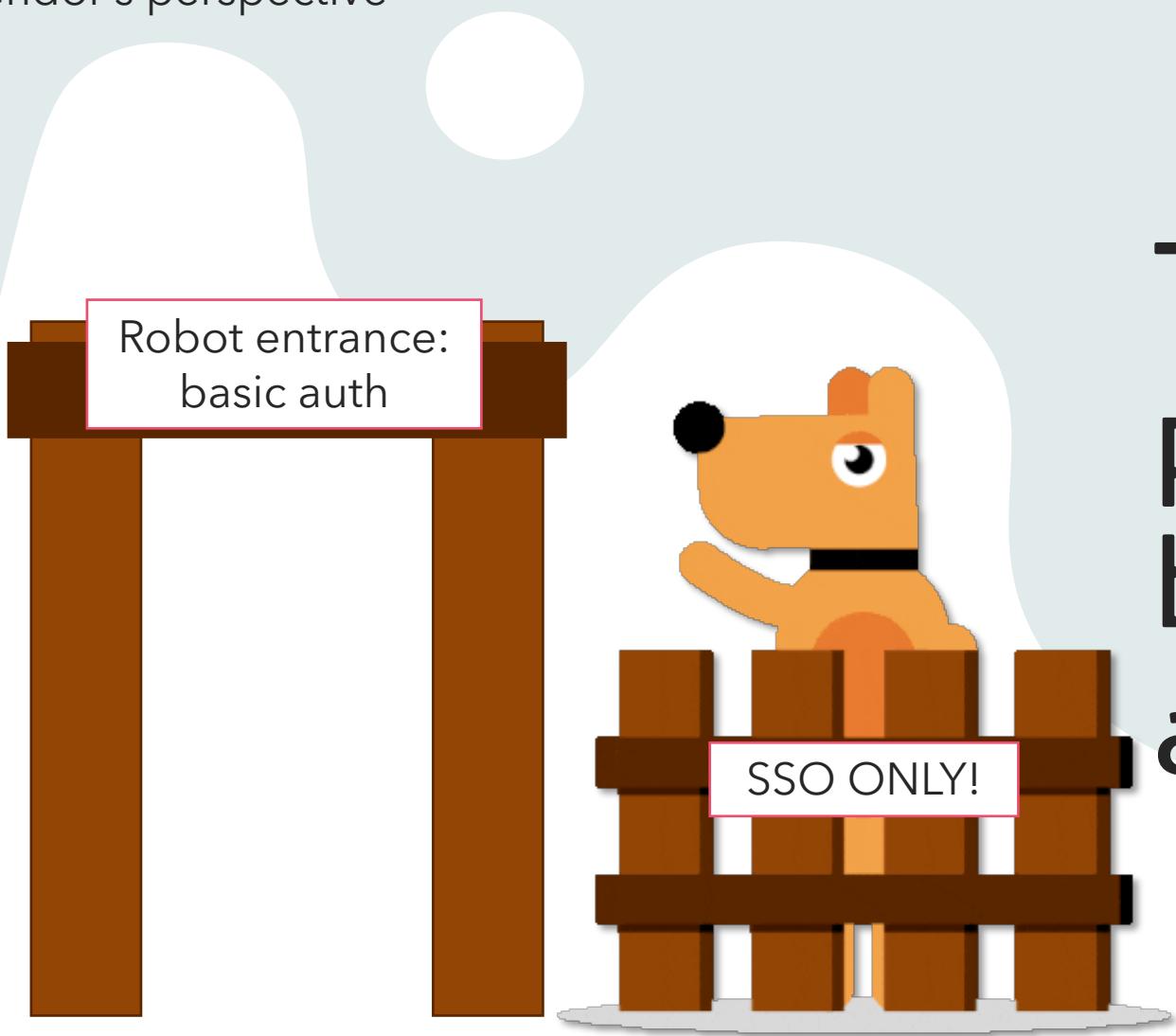
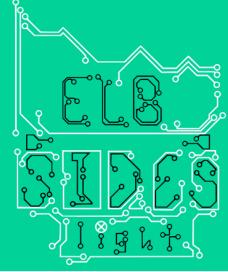
They might let  
users change  
their own info



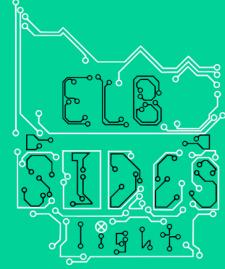
**Useful Shared**  
account

Bob, **Aiwang**, or  
**Cheech**

They might have  
good reasons to  
have different  
rules

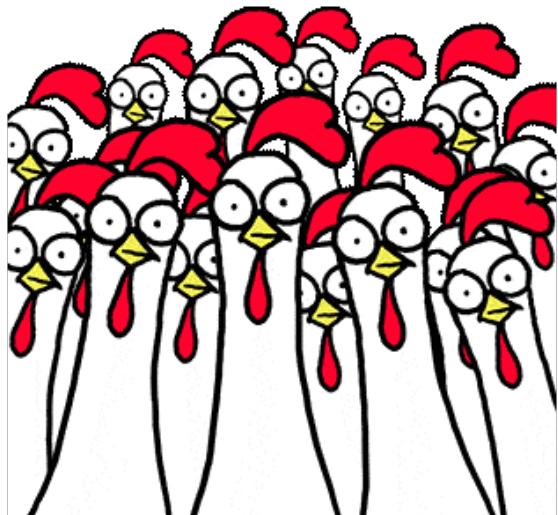


There might be  
places where  
basic auth is still  
available



# So now we know what we need, and what the **vendor** can do

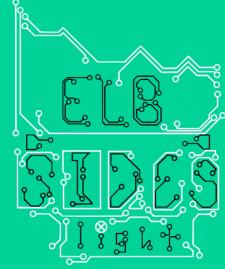
Vendor accounts



Your company accounts



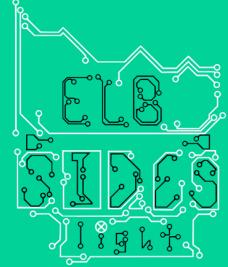
How to translate  
between chickens  
and broccoli???



# ASK QUESTIONS

don't just assume!





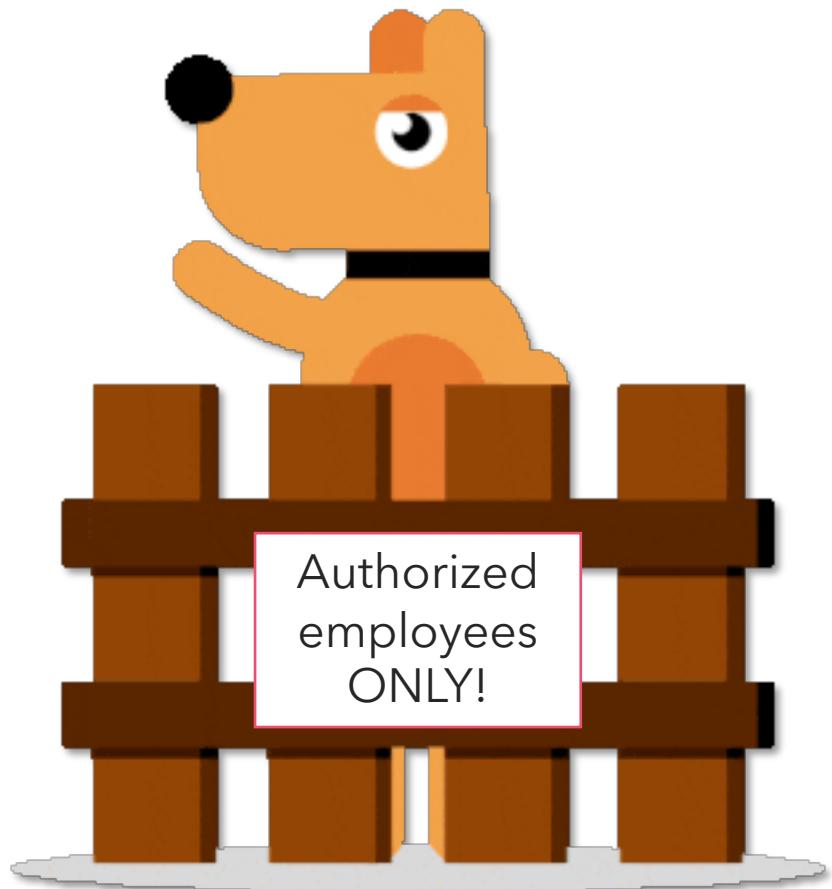
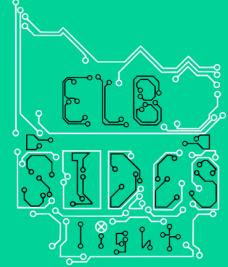
# Why am I giving this talk?

## Step 2: **OMG WTF SSO**

- What do I actually **need**?
- **What** can my vendor **do**?
- **Ask weird questions:**  
communication is hard and  
people make mistakes

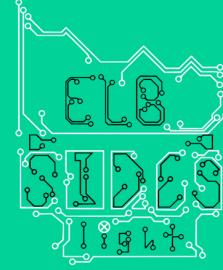
Me, **now**





## Need #1: Use **my** authentication

- a) Only** use **my** authentication
- b) Force** use of SSO



# Weird questions about a) Only use my authentication

Is there a way that someone authenticating to a  
**different identity provider** could get into one of  
**my org's accounts?**



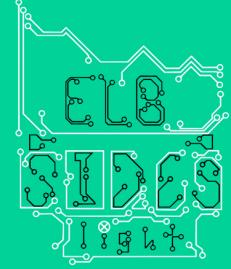
# Failure case

Turning “sso on” for your org’s accounts still allows **anyone else** with:

- Any random identity in any **other SSO setup connected to the vendor**
- The **username/password** for any of **your org’s vendor accounts**

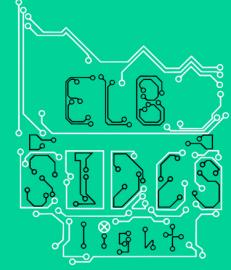
to **link their ID** to **your** org’s vendor account.

**Nobody gets notified** (not you, not the user)



# Weird questions about b) Force use of SSO

- Will you ever fail over away from my authentication?
- What access is enforced for API users?



# Failure case

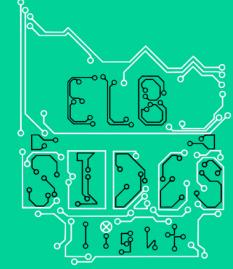


The vendor has:

- **enforced SSO** using the **user interface**,
- Given me **control** over how **API** users authenticate

But...

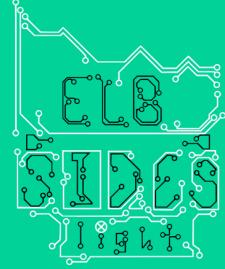
Their own app can't use SSO



## Need #2: Users can **only** access their **own** stuff

- a) Bob\* can **only** access **Bob's** vendor **account**
- b) I don't want **shared accounts**

\* Authenticated to Bob's ID with my identity provider



# Weird questions about a) Bob\* can **only** access **Bob's** **vendor account**

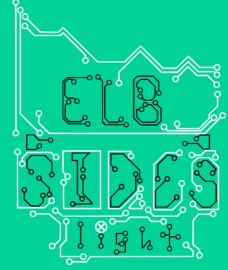
If **Bob** has the **credentials** for **Alice's vendor account**, can he access Alice's account too?

Does the **attribute mapping** rely on **non-user-editable** fields?

You do have **attribute mapping**, right?

What happens if I **change everything** possible on my account? Can I still get in?

\* Authenticated to Bob's ID with my identity provider



# Failure case

**Attribute mapping** wasn't in the **MVP**.

The vendor just made a big ol' lookup table of **usernames** linked to UDPs of the linked IdP.

Vendor account username is **editable by the user**.





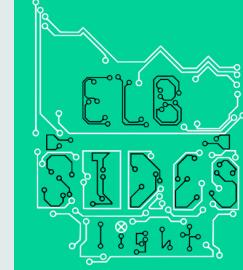
Achievement unlocked

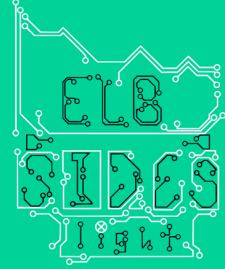


# Failure case

Attack unlocked!

- 1. Make an account** in your org with a **username** you think **your competitor** will use
- 2. Link** that to one of **your identities**
- 3. Change** the username
- 4. Competitor makes account** with username
- 5. You can get in** to that account and no-one will know

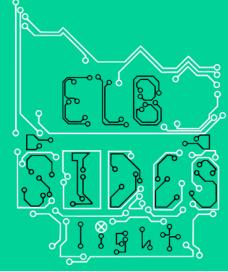




# Weird questions about b) I don't want **shared accounts**

How has the vendor designed shared accounts to work?

Are they SURE they don't allow them? Not anywhere?

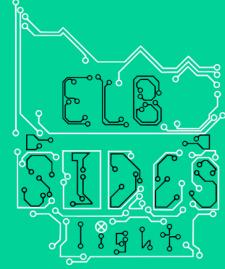


# Failure case

A close-up photograph of a white plate filled with spaghetti. The pasta is coated in a rich, red tomato sauce and topped with finely grated white cheese and several large, fresh green basil leaves. The plate is set against a plain, light-colored background.

You didn't ask, but they do offer shared accounts...

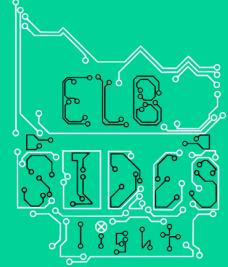
All it takes is the second user signing in with their own authenticated identity and the vendor account's username and password.



# What's the point?

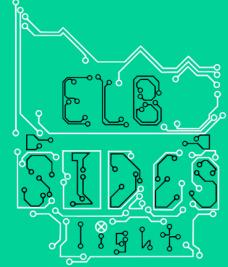
Misconfiguration is nothing new!

This talk is boring and nobody needs it because there are a million ways to fail, just do it right!



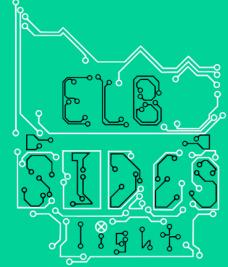
# What's the point?

Your colleagues and managers who work with vendors **might not know** that messing this up is easy and common.



# What's the point?

**Empower** your **colleagues**, and **yourself** to **ask questions** and not make assumptions!



**So please,  
ask me questions!**

- Adina Bogert-O'Brien
- <https://discontinuity.ca/>

